

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

3284 N. Sherman Boulevard, Apartment 2, Milwaukee,
Wisconsin

)
)
)
)
)
)

Case No. 16-M-1317

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

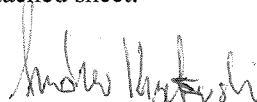
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. 844(i) Malicious Use of Fire

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Andrew Krzeptowski, ATF

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 9/21/16



Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Andrew Krzeptowski, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, a residential dwelling described in Attachment A, and the extraction from that property of evidence described in Attachment B.

2. I am employed with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been so employed since September of 2014. I attended the Federal law Enforcement Training Center where I completed both the Criminal Investigator Training Program and the ATF Special Agent Basic Training program. My duties as a Special Agent with ATF include investigating alleged violations of the federal firearms, arson, and explosives laws under the purview of the Gun Control Act (as amended) under Title 18 of the United States Code.

3. As part of my duties as an ATF Special Agent, I investigate criminal violations relating to violent crime, and firearms and explosives offenses, including 18 U.S.C. 922(g)(1) (felon in possession of a firearm), 18 U.S.C. 924(c) (use of a Molotov Cocktail to commit a federal arson crime) and 26 U.S.C. 5861(d), (e) & (f), (possess, transfer or making a firearm not registered in the National Firearms Registration and Transfer Record).

4. This affidavit is made in support of an application for a warrant to search the residence of Charles N. Edwards located at 3284 N. Sherman Boulevard, Apartment 2, Milwaukee, Wisconsin, 53216. The search will be for a laptop computer containing evidence associated with violations of Title 26 United States Code 5861 (d) illegally possessing or receiving a firearm which is not registered to him in the National Firearms Registration and Transfer Record (NFRTR), 18

U.S.C. 924(c) use of a Molotov Cocktail to commit a federal arson crime and Title 18 United States Code 922 (g) (1) illegal possession of a firearm by a convicted felon. In the below affidavit, the firearms are described in Title 18 United States Code 921 (D) any destructive device, further described under Title 18 United States Code 921 (4) (A) as a destructive device means any explosive, incendiary, or poison gas. The firearms in question in this affidavit is also described in Title 26 United States Code 5845 (f) (1) as any destructive device which means any explosive, incendiary, or poison gas.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF PREMISE TO BE SEARCHED

6. The property to be searched is 3284 N. Sherman Boulevard, Apartment 2, Milwaukee, Wisconsin (PREMISES), described as a tan colored apartment. Apartment 2 is described as a first story unit with a deck that has a door to enter the unit. The siding and deck railing appear tan in color. The front door of the unit is a yellow woodgrain, with a black placard affixed to it displaying the number "2" in white. The door is further comprised of a silver-colored peephole, silver-colored door handle, and silver-colored dead bolt lock. The trim around the door is black.

7. The applied-for warrant would authorize the search and recovery of evidence particularly described in Attachment B.

PROBABLE CAUSE

8. On the night of August 13, 2016, and continuing into the morning of August 14, 2016, the city of Milwaukee experienced civil unrest that resulted in numerous arsons. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) initiated multiple investigations into suspected arsons against businesses engaged in interstate commerce as set forth under Title 18 United States Code 844 (i). As a result of the aforementioned investigation, the ATF and law enforcement conducted and documented multiple witness interviews that indicated the use and possession of "Molotov Cocktails" during the above dates.

9. On August 16, 2016, the Milwaukee, Wisconsin, Police Department (MPD) recovered a glass bottle containing a liquid with a torn black cloth stuffed inside the bottle at 3284 N. Sherman Boulevard, Milwaukee, Wisconsin. I know from training and experience the aforementioned construction is consistent with the destructive device known as a "Molotov Cocktail" and herein referred to as a Molotov Cocktail.

10. On August 23, 2016, ATF was contacted regarding suspected Improvised Incendiary Devices (IID) located within a dumpster at 3284 N. Sherman Boulevard, Milwaukee, Wisconsin. ATF Special Agents traveled to the above location and discovered a brown box containing ten glass bottles containing a liquid with a cloth rag inserted into the opening. The responding agents also smelled a strong odor of a petroleum distillate emanating from the dumpster, which is consistent with the presence of gasoline. The agents identified these devices as suspect Molotov Cocktails from training and experience. Some of the glass bottles holding the liquid and cloth wick were labeled as Mike's Hard Lemonade, Everfresh juice, Mystic, and Seagrams Wine Coolers.

11. The building manager for 3284 N. Sherman Blvd., Milwaukee, WI, Jerome Mommaers, gave to law enforcement two apartment complex surveillance videos from August 15, 2016 and August 16, 2016.

12. Affiant is aware of the contents of those videos. The first video shows, on August 16, 2016, an unknown person who appears to drop off an item in the location where officers recovered a single Molotov Cocktail on August 16, 2016. The second video shows, on August 15, 2016, an unknown person who is carrying a brown box by the dumpster next to the apartment complex, which is consistent to where officers recovered a brown box containing multiple Molotov Cocktails on August 23, 2016.

13. The above-referenced apartment complex videos show that both unknown persons walked in the area by Charles N. Edwards' apartment, which is unit #2. Through the apartment manager at 3284 N. Sherman Blvd., Milwaukee, affiant received information that the apartment manager has personal knowledge that a tenant, Charles N. Edwards, currently has video surveillance devices that appear to capture activity on the outside of his apartment unit. It is believed that Charles N. Edwards' video surveillance system captured the unknown persons suspected of possessing Molotov Cocktails on August 15, 2016 and August 16, 2016 at 3284 N. Sherman Blvd., Milwaukee, WI.

14. On August 23, 2016, and while still on location at 3284 N. Sherman Boulevard, Milwaukee, Wisconsin, ATF Special Agents observed a nozzle for a gas can under the porch of 3284 N. Sherman Boulevard, Apartment 2, Milwaukee, WI. Agents spoke with the resident of this unit who was ultimately identified as Charles N. Edwards of 3284 N. Sherman Boulevard, Apartment 2, Milwaukee, WI. Edwards explained to agents that this nozzle was part of a gas can he had for a generator.

15. On August 26th, 2016, a juvenile Source of Information (SOI) was interviewed by ATF Special Agents regarding the fires started during the night of August 13, 2016, and morning of August 14, 2016. The SOI stated that they observed a subject light and throw a Molotov Cocktail into the BP Gas Station located at 3114 N. Sherman Boulevard, Milwaukee, Wisconsin and pour flammable liquids onto the vehicles located at the BP gas station. SOI said this subject was then joined by two additional males who threw additional Molotov Cocktails into the gas station.

16. On August 29, 2016, law enforcement conducted a search warrant at the residence of Van L. Mayes located at 2746 A, North 49th Street, Milwaukee, Wisconsin. Law enforcement observed a full bottle of a Seagram's Wine Cooler and one empty bottle of Everfresh juice consistent with the type used in the construction of the Molotov Cocktails recovered by law enforcement on August 23, 2016, from the dumpster of 3284 N. Sherman Boulevard, Milwaukee, Wisconsin. During the search warrant, Mayes related to law enforcement that two gasoline cans and empty bottles from his house were transported to a man named Charles who used a wheelchair and resided off of Sherman. Mayes further stated that he took possession of a generator from Charles after the above interaction with ATF but left the two cans of gasoline at Charles' residence.

17. Affiant verified that Charles N. Edward is currently in a wheelchair.

18. On August 30, 2016, ATF Special Agents were directed by the building technician of 3114 N. Sherman Boulevard, Milwaukee, Wisconsin, to the Apartment No. 2 as the unit currently inhabited by Charles N. Edwards. Subsequently, ATF Agents reviewed a spreadsheet provided by building management of current tenants listed Apartment No. 2 as inhabited by Charles N. Edwards.

19. An inquiry into the National Firearm Registration and Transfer Record revealed that Charles N. Edwards was not on record.

20. An inquiry into the criminal history of Charles N. Edwards shows he was convicted of a felony, burglary, on March 5, 1998, thus making him a convicted felon.

21. On August 29, 2016, the Milwaukee Police Department arrested Charles N. Edwards for possession with intent to deliver cocaine base, while armed with a handgun, in violation of Wis. Stat. § 961.41.

22. On August 30, 2016, Milwaukee County Court Judge Timothy Witkowiak signed a search warrant for Charles N. Edwards' residence located at 3284 N. Sherman Boulevard Apartment #2, Milwaukee, Wisconsin to search for evidence of narcotics and guns.

23. During the search of Charles N. Edwards' residence, the Milwaukee Police Department located gas cans inside of a bedroom; a gas can nozzle within the apartment's yard; and Everfresh juice, Seagrams Wine Cooler, Mystic bottle caps within his trash receptacle on the outside of his apartment's porch, but no bottles.

24. On August 30, 2016, the Honorable Nancy Joseph, United States Magistrate Judge in the Eastern District of Wisconsin, signed a search warrant for Charles N. Edwards' residence and media devices.

25. On August 30, 2016, ATF Agents conducted a search warrant at Charles N. Edwards' residence located at 3284 N. Sherman Blvd., Milwaukee. During the execution of this search warrant, media storage device evidence relating to the security cameras in Edwards' residence, which is suspected to contain evidence pertaining to violations of 18 U.S.C. § 922(g)(1) (felon in possession of a firearm) and 26 U.S.C. §§ 5861(d), (e) & (f), (possess, transfer or making a firearm not registered in the National Firearms Registration and Transfer Record), was seized.

26. An examinitaion of the security camera devices showed that they can be connected to a desktop or a laptop computer. The desktop or laptop computer may then record the footage captured by the security camera devices

27. During the search of Charles N. Edwards' residence, Samantha Gamble (B/F, DOB:10/21/1976), step daughter of Edwards, stated she lived with Edwards. Gamble explained that on August 29, 2016, "people" from Sherman park came to her residence at approximately 1:00 pm and took Edwards' laptop computer. When asked whether security cameras inside her unit backed up onto the missing laptop, Gamble stated she did not know.

28. On August 19, 2016, ATF SAs reviewed recordings of phone calls placed by Charles Edwards from Milwaukee County jail in regards to the laptop computer.

29. Phone call 116043069 was placed to phone number 414-488-2621 listing to Samantha Gamble, (B/F 10-21-1976), step daughter of Edwards. At approximately 04:10 of the call, Edwards asks Gamble what the police took during the search warrant at his residence. At approximately 04:20, Gamble states "they asked me where your laptop was at, I told them it wasn't here."

30. Phone call 116109770 was placed to phone number 414-304-9086 listing to Gamble. An individual with a female voice answers, but does not sound like Gamble from earlier jail calls. At approximately 02:40 of the phone call, a female voice informs Edwards that "GC" said she had passed the laptop off to "V" and that she is supposed to meet "V" at the park to get it. Edwards than replies to keep that "hush."

31. Phone call 116139490 was placed to phone number 414-488-2621 listing to Gamble. An individual with a child's voice answers. During the phone call, Edwards converses with the child in regards to the search warrant executed at his residence. At approximately 09:39

of the phone call the child explains to Edwards that law enforcement officers took Edwards laptop. Edwards replies that law enforcement officers did not take his laptop computer as it wasn't at his residence

32. On September 21, 2016 at approximately 12:49pm, ATF Agents Hankins and Rorabeck returned property which was seized during a search warrant on August 30, 2016, to Edwards at his residence located at 3284 N Sherman, Apt# 2, Milwaukee, WI. ATF Agents approached Edwards and Samantha Gamble at the front door and informed Gamble they had Edwards' property to return. Gamble led Agents to Edwards' apartment, unlocked the door, and held the door open for Agents to enter. Agent Rorabeck and Hankins entered with Edwards' property and the return of property receipt. Agent Rorabeck placed Edwards' items on a living room table. While in the living room, Agent Hankins could see into Edwards' bedroom. ATF agents identified this as Edwards' bedroom from the recent and prior search warrant on August 30, 2016. Agent Hankins saw, in plain view, a laptop computer on top of a shelf in Edwards' bedroom. Edwards' laptop computer is more fully described as a Dell brand that is black and silver in color.

33. Affiant believes that the laptop computer's storage systems were used to record Edwards' security camera footage, which likely captured the events of August 13, 2016 through August 16, 2016 and may be evidence of the violations of 18 U.S.C. § 922(g)(1) (felon in possession of a firearm) and 26 U.S.C. §§ 5861(d), (e) & (f), (possess, transfer or making a firearm not registered in the National Firearms Registration and Transfer Record).

34. Through the Affiant's knowledge, training and experience, and the experience of other law enforcement personnel, he knows also knows that computers are used for research purposes and the searches and webpages looked at are saved within the computer's storage

systems, and Edwards' computer may show evidence of researching how to build Molotov cocktails, which is evidence of violations of 18 U.S.C. § 922(g)(1) (felon in possession of a firearm) and 26 U.S.C. §§ 5861(d), (e) & (f), (possess, transfer or making a firearm not registered in the National Firearms Registration and Transfer Record).

35. Affiant believes that Edwards' laptop holds data with evidence of the violations of 18 U.S.C. § 922(g)(1) (felon in possession of a firearm) and 26 U.S.C. §§ 5861(d), (e) & (f), (possess, transfer or making a firearm not registered in the National Firearms Registration and Transfer Record).

36. Based upon affiant's knowledge, training and experience, and the experience of other law enforcement personnel, he knows that searches and seizures of evidence from cameras, computer related hardware, external memory or storage devices, and computers commonly require officers to seize the portable electronic devices and computers described above to be processed later by a qualified computer expert.

37. Computer storage devices (like hard drives, diskettes, tapes, laser disks, USB devices and others) can store the equivalent of thousands of pages of information. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

38. In order to locate images or video files, affiant knows that a forensic preview of a suspect hard drive or other storage device can take place at the scene of a search; however, this preliminary search does not necessarily find all evidence about the nature and scope of the crime being investigated. Searching computer systems for all obtainable evidence is a highly technical process that requires expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some

systems and applications. A search of a camera, phone or computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files.

39. Affiant is aware that the film documentarians commonly collect raw footage both before, during, and after video shoots and later utilize equipment of various types to amalgamate the raw footage into a video that is later distributed for viewing.

40. Affiant is aware that the process of editing a videos can be a time consuming process and that videographers and documentarians commonly retain source footage for considerable lengths of time, including postproduction.

41. Affiant is aware that the producers of such videos commonly store footage on various types of media, to include film (developed and undeveloped), digital media (including but not limited to memory cards, memory sticks, computers/computer hard drives, optical media such as CD's and DVD's, and electronic devices such as cell phones and/or tablets, as well as cloud storage, where data is stored off-site in a digital cloud and accessible to the user(s) via computer or electronic device). Affiant is also aware that content may be stored upon the device that performed the recording and such devices can include cameras, cellular phones, video cameras, etc.

42. Affiant is aware that the portability of various media types, including digital media, makes the items easy to transport or carry, and may be located in various locations, including a subject's automobile or person in addition to their home or business.

43. Affiant is further aware that video and images stored electronically can be easily destroyed by deletion and/or the use of specialized software.

44. Affiant believes that footage from the aforementioned videos, both raw and production level footage, will assist investigators in investigating the suspected violations of 18 U.S.C. § 922(g)(1) (felon in possession of a firearm) and 26 U.S.C. §§ 5861(d), (e) & (f), (possess, transfer or making a firearm not registered in the National Firearms Registration and Transfer Record).

TECHNICAL TERMS

45. Specifically, affiant believes that Edwards' laptop and video footage will assist in supporting the criminal charges of the individuals previously described and aide in their prosecution. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and

international borders, even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

46. As described above and in Attachment B, this application seeks permission to seize the laptop computer located at the PREMISES. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. *Probable cause.* I submit that if a laptop computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that laptop computer or storage medium, for at least one of the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

48. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only the laptop computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

49. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

50. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage

media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

51. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

52. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

53. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

54. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

55. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a

computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

56. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

57. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

58. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted

scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

59. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of the laptop computer or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

60. I submit that this affidavit supports probable cause for a search warrant authorizing the search of 3284 N. Sherman Boulevard, Apartment 2, Milwaukee, Wisconsin, fully described in Attachment A. Additionally, I submit that this affidavit supports probable cause to seek the items described in Attachment B.

ATTACHMENT A

Property to Be Searched

3284 N. Sherman Boulevard, Apartment 2, Milwaukee, Wisconsin, herein described as a tan colored apartment. Apartment 2 is described as a first story unit with a deck that has a door to enter the unit. The siding and deck railing appear tan in color. The apartment door is a yellow woodgrain with a black affixed placard displaying the number "2" on it. The door also has a silver peephole, silver dead bolt lock, and silver handle. There is a black trip around the door.

ATTACHMENT B

Particular Things to be Seized

- Laptop Computer
 - Edwards' laptop computer is more fully described as a Dell brand that is black and silver in color;
 - Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media;
 - Computer storage media used for this laptop such as the digital content to include but not limited to SD cards, micro SD cards, external "thumb" or "jump" or removable drive, floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images;
- Laptop Computer software and application software installation and operation media
 - Laptop computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address;
 - Manuals and other documents (whether digital or written), which describe operation of items or software, seized;
 - Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized;

- Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images and depictions pertaining to the aforementioned crimes;
 - Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to produce the aforementioned media, to include credit card bills, telephone bills, correspondence and other identification documents; and
 - Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.
- For the laptop computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- evidence of the lack of such malicious software;
- evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- evidence of the times the COMPUTER was used;
- passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- records of or information about Internet Protocol addresses used by the COMPUTER;
- records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- contextual information necessary to understand the evidence described in this attachment.

- Routers, modems, and network equipment used to connect computers to the Internet.
- As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
- The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
- The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.